

Post-Quantum Cryptography Market Forecasts to 2034 – Global Analysis By Offering (Solutions and Services), Algorithm Type, Deployment Mode, End User and By Geography

<https://marketpublishers.com/r/P30465274F80EN.html>

Date: April 2026

Pages: 200

Price: US\$ 4,150.00 (Single User License)

ID: P30465274F80EN

Abstracts

According to Statistics MRC, the Global Post-Quantum Cryptography Market is accounted for \$0.7 billion in 2026 and is expected to reach \$19.2 billion by 2034, growing at a CAGR of 49.5% during the forecast period. Post-Quantum Cryptography (PQC) is a field of cryptography focused on developing encryption methods capable of resisting attacks from quantum computers. Traditional cryptographic systems may become vulnerable once large-scale quantum computing becomes practical. PQC uses mathematical problems that are considered difficult for both classical and quantum computers to solve. These algorithms are designed to run on existing computing systems and communication networks while providing protection against quantum-based threats, ensuring that sensitive data and digital communications remain secure in the future.

Market Dynamics:

Driver:

Growing threat of quantum decryption

Quantum machines using Shor's algorithm can theoretically break these protocols within hours, exposing global digital infrastructure. Governments and enterprises are accelerating PQC adoption to safeguard sensitive data against future harvest-now-decrypt-later attacks. Increasing investments in national quantum initiatives and post-quantum roadmaps are compelling organizations to upgrade cryptographic assets. The

urgency is further amplified by data retention regulations, as stolen encrypted data today could be decrypted by future quantum systems, making proactive migration to PQC a strategic imperative for long-term security.

Restraint:

High migration complexity and costs

Transitioning from classical to post-quantum cryptography involves overhauling legacy systems, hardware modules, and communication protocols. Enterprises face significant technical challenges in integrating PQC algorithms without disrupting existing operations. Smaller organizations struggle with the financial burden of cryptographic audits, staff retraining, and system upgrades. Additionally, hybrid cryptographic modes that run classical and PQC algorithms in parallel demand higher computational resources. These constraints slow down mass adoption, particularly in industries with legacy-dependent operational technology environments.

Opportunity:

Government mandates and compliance requirements

Regulatory bodies worldwide are issuing guidelines and deadlines for quantum-safe migration. The U.S. National Institute of Standards and Technology (NIST) has finalized PQC standards, while the EU and other regions are developing similar frameworks. Compliance with directives such as the EU Cybersecurity Act and U.S. Quantum Computing Cybersecurity Preparedness Act is forcing public and private sectors to adopt PQC solutions. This regulatory push creates a multi-billion-dollar opportunity for vendors offering migration tools, consulting, and managed services. Early adopters gain competitive advantage by demonstrating quantum readiness, while technology providers can bundle PQC with existing security suites to accelerate market penetration.

Threat:

Immature standards and algorithm vulnerabilities

Although NIST has standardized several PQC algorithms, the field remains relatively young compared to classical cryptography. New cryptanalysis techniques continue to uncover potential vulnerabilities in lattice-based, code-based, and multivariate schemes. The risk of undiscovered backdoors or mathematical weaknesses poses a serious

threat to long-term trust in PQC solutions. Furthermore, hardware acceleration for PQC is not yet widespread, leading to latency issues in high-throughput environments. Organizations may delay adoption until algorithms mature further, creating a window of exposure. Without continuous monitoring and agile cryptographic agility, early adopters could face costly re-migrations if selected algorithms are compromised.

Covid-19 Impact

The pandemic accelerated digital transformation, expanding attack surfaces across remote work, telehealth, and cloud services. This surge in data exchange heightened awareness of long-term cryptographic risks, including quantum threats. However, budget reallocations toward immediate pandemic response delayed some PQC research and pilot projects. Supply chain disruptions affected hardware security module availability for cryptographic testing. Conversely, government stimulus packages included cybersecurity modernization funds, indirectly supporting PQC readiness. Post-pandemic strategies now emphasize cryptographic agility, with organizations integrating PQC into zero-trust architectures and long-term data protection plans, recognizing quantum resilience as a critical business continuity factor.

The solutions segment is expected to be the largest during the forecast period

The solutions segment is expected to account for the largest market share, driven by immediate demand for quantum-resistant encryption tools, key management systems, and secure communication platforms. Enterprises are prioritizing software libraries and hardware modules that replace vulnerable RSA and ECC implementations. Encryption tools enable data-at-rest and in-transit protection, while key management ensures secure cryptographic lifecycle governance. Digital signatures based on PQC algorithms prevent forgery in legal and financial transactions.

The BFSI segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the BFSI segment is predicted to witness the highest growth rate, driven by the need to protect long-lived financial data, transaction integrity, and payment systems. Banks and insurance firms face significant risks from harvest-now-decrypt-later attacks on wire transfers, customer records, and blockchain assets. Regulatory pressure from central banks and financial authorities is accelerating PQC pilots and migrations. Integration of quantum-safe algorithms into ATMs, online banking platforms, and interbank settlement systems is rising.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, fuelled by aggressive government initiatives from NIST and the Department of Homeland Security. The United States leads in PQC standardization, research funding, and early adoption across defense, finance, and cloud sectors. Presence of major technology vendors and cryptographic startups accelerates product commercialization. Strong collaboration between national labs, universities, and private enterprises drives algorithm development and testing.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, supported by rapid digitalization and growing quantum computing research in China, Japan, India, and South Korea. Governments are launching national quantum missions and post-quantum migration roadmaps to protect critical infrastructure. Increasing cross-border data flows and cyber threats from state-sponsored actors drive urgency for PQC adoption. Expanding BFSI, telecom, and e-commerce sectors seek quantum-safe solutions for long-term data protection.

Key players in the market

Some of the key players in Post-Quantum Cryptography Market include IBM Corporation, Microsoft Corporation, Amazon Web Services, NXP Semiconductors, Thales Group, IDEMIA, Palo Alto Networks, DigiCert, PQShield, Post?Quantum Ltd., ISARA Corporation, QuintessenceLabs, Quantum Xchange, Keyfactor, and QuSecure.

Key Developments:

In March 2026, IBM and ETH Zurich announced a 10-year collaboration to advance the next generation of algorithms at the intersection of AI and quantum computing. This initiative represents the latest milestone in the long-standing collaboration between the two institutions, further strengthening a scientific exchange that has helped create the future of information technology.

In March 2026, Thales partners with Service Oklahoma to launch next-generation driver licenses and ID cards. Service Oklahoma has selected Thales to deliver new driver licenses and ID cards designed for maximum security, durability, and sustainability. The new credentials are made from 100% polycarbonate, a durable material that embeds

advanced security features to prevent fraud.

Offerings Covered:

Solutions

Services

Algorithm Types Covered:

Lattice- based

Code? based

Multivariate

Hash? based

Isogeny? based

Deployment Modes Covered:

On?Premises

Cloud

End Users Covered:

BFSI

Government & Defense

IT & Telecom

Healthcare

Retail & eCommerce

Manufacturing

Energy & Utilities

Other End Users

Regions Covered:

North America

United States

Canada

Mexico

Europe

United Kingdom

Germany

France

Italy

Spain

Netherlands

Belgium

Sweden

Switzerland

Poland

Rest of Europe

Asia Pacific

China

Japan

India

South Korea

Australia

Indonesia

Thailand

Malaysia

Singapore

Vietnam

Rest of Asia Pacific

South America

Brazil

Argentina

Colombia

Chile

Peru

Rest of South America

Rest of the World (RoW)

Middle East

Saudi Arabia

United Arab Emirates

Qatar

Israel

Rest of Middle East

Africa

South Africa

Egypt

Morocco

Rest of Africa

What our report offers:

Market share assessments for the regional and country-level segments

Strategic recommendations for the new entrants

Covers Market data for the years 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032 and 2034

Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)

Strategic recommendations in key business segments based on the market estimations

Competitive landscaping mapping the key common trends

Company profiling with detailed strategies, financials, and recent developments

Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

Contents

1 EXECUTIVE SUMMARY

- 1.1 Market Snapshot and Key Highlights
- 1.2 Growth Drivers, Challenges, and Opportunities
- 1.3 Competitive Landscape Overview
- 1.4 Strategic Insights and Recommendations

2 RESEARCH FRAMEWORK

- 2.1 Study Objectives and Scope
- 2.2 Stakeholder Analysis
- 2.3 Research Assumptions and Limitations
- 2.4 Research Methodology
 - 2.4.1 Data Collection (Primary and Secondary)
 - 2.4.2 Data Modeling and Estimation Techniques
 - 2.4.3 Data Validation and Triangulation
 - 2.4.4 Analytical and Forecasting Approach

3 MARKET DYNAMICS AND TREND ANALYSIS

- 3.1 Market Definition and Structure
- 3.2 Key Market Drivers
- 3.3 Market Restraints and Challenges
- 3.4 Growth Opportunities and Investment Hotspots
- 3.5 Industry Threats and Risk Assessment
- 3.6 Technology and Innovation Landscape
- 3.7 Emerging and High-Growth Markets
- 3.8 Regulatory and Policy Environment
- 3.9 Impact of COVID-19 and Recovery Outlook

4 COMPETITIVE AND STRATEGIC ASSESSMENT

- 4.1 Porter's Five Forces Analysis
 - 4.1.1 Supplier Bargaining Power
 - 4.1.2 Buyer Bargaining Power
 - 4.1.3 Threat of Substitutes
 - 4.1.4 Threat of New Entrants

- 4.1.5 Competitive Rivalry
- 4.2 Market Share Analysis of Key Players
- 4.3 Product Benchmarking and Performance Comparison

5 GLOBAL POST-QUANTUM CRYPTOGRAPHY MARKET, BY OFFERING

- 5.1 Solutions
 - 5.1.1 Encryption Tools
 - 5.1.2 Key Management
 - 5.1.3 Secure Communication
 - 5.1.4 Digital Signatures
- 5.2 Services
 - 5.2.1 Consulting
 - 5.2.2 Integration & Deployment
 - 5.2.3 Support & Maintenance

6 GLOBAL POST-QUANTUM CRYPTOGRAPHY MARKET, BY ALGORITHM TYPE

- 6.1 Lattice based
- 6.2 Code based
- 6.3 Multivariate
- 6.4 Hash based
- 6.5 Isogeny based

7 GLOBAL POST-QUANTUM CRYPTOGRAPHY MARKET, BY DEPLOYMENT MODE

- 7.1 On Premises
- 7.2 Cloud
 - 7.2.1 Public Cloud
 - 7.2.2 Private Cloud
 - 7.2.3 Hybrid Cloud

8 GLOBAL POST-QUANTUM CRYPTOGRAPHY MARKET, BY END USER

- 8.1 BFSI
- 8.2 Government & Defense
- 8.3 IT & Telecom
- 8.4 Healthcare

- 8.5 Retail & eCommerce
- 8.6 Manufacturing
- 8.7 Energy & Utilities
- 8.8 Other End Users

9 GLOBAL POST-QUANTUM CRYPTOGRAPHY MARKET, BY GEOGRAPHY

- 9.1 North America
 - 9.1.1 United States
 - 9.1.2 Canada
 - 9.1.3 Mexico
- 9.2 Europe
 - 9.2.1 United Kingdom
 - 9.2.2 Germany
 - 9.2.3 France
 - 9.2.4 Italy
 - 9.2.5 Spain
 - 9.2.6 Netherlands
 - 9.2.7 Belgium
 - 9.2.8 Sweden
 - 9.2.9 Switzerland
 - 9.2.10 Poland
 - 9.2.11 Rest of Europe
- 9.3 Asia Pacific
 - 9.3.1 China
 - 9.3.2 Japan
 - 9.3.3 India
 - 9.3.4 South Korea
 - 9.3.5 Australia
 - 9.3.6 Indonesia
 - 9.3.7 Thailand
 - 9.3.8 Malaysia
 - 9.3.9 Singapore
 - 9.3.10 Vietnam
 - 9.3.11 Rest of Asia Pacific
- 9.4 South America
 - 9.4.1 Brazil
 - 9.4.2 Argentina
 - 9.4.3 Colombia

- 9.4.4 Chile
- 9.4.5 Peru
- 9.4.6 Rest of South America
- 9.5 Rest of the World (RoW)
 - 9.5.1 Middle East
 - 9.5.1.1 Saudi Arabia
 - 9.5.1.2 United Arab Emirates
 - 9.5.1.3 Qatar
 - 9.5.1.4 Israel
 - 9.5.1.5 Rest of Middle East
 - 9.5.2 Africa
 - 9.5.2.1 South Africa
 - 9.5.2.2 Egypt
 - 9.5.2.3 Morocco
 - 9.5.2.4 Rest of Africa

10 STRATEGIC MARKET INTELLIGENCE

- 10.1 Industry Value Network and Supply Chain Assessment
- 10.2 White-Space and Opportunity Mapping
- 10.3 Product Evolution and Market Life Cycle Analysis
- 10.4 Channel, Distributor, and Go-to-Market Assessment

11 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES

- 11.1 Mergers and Acquisitions
- 11.2 Partnerships, Alliances, and Joint Ventures
- 11.3 New Product Launches and Certifications
- 11.4 Capacity Expansion and Investments
- 11.5 Other Strategic Initiatives

12 COMPANY PROFILES

- 12.1 IBM Corporation
- 12.2 Microsoft Corporation
- 12.3 Amazon Web Services (AWS)
- 12.4 NXP Semiconductors
- 12.5 Thales Group
- 12.6 IDEMIA

- 12.7 Palo Alto Networks
- 12.8 DigiCert
- 12.9 PQShield
- 12.10 Post Quantum Ltd.
- 12.11 ISARA Corporation
- 12.12 QuintessenceLabs
- 12.13 Quantum Xchange
- 12.14 Keyfactor
- 12.15 QuSecure

List Of Tables

LIST OF TABLES

Table 1 Global Post-Quantum Cryptography Market Outlook, By Region (2023-2034) (\$MN)

Table 2 Global Post-Quantum Cryptography Market Outlook, By Offering (2023-2034) (\$MN)

Table 3 Global Post-Quantum Cryptography Market Outlook, By Solutions (2023-2034) (\$MN)

Table 4 Global Post-Quantum Cryptography Market Outlook, By Encryption Tools (2023-2034) (\$MN)

Table 5 Global Post-Quantum Cryptography Market Outlook, By Key Management (2023-2034) (\$MN)

Table 6 Global Post-Quantum Cryptography Market Outlook, By Secure Communication (2023-2034) (\$MN)

Table 7 Global Post-Quantum Cryptography Market Outlook, By Digital Signatures (2023-2034) (\$MN)

Table 8 Global Post-Quantum Cryptography Market Outlook, By Services (2023-2034) (\$MN)

Table 9 Global Post-Quantum Cryptography Market Outlook, By Consulting (2023-2034) (\$MN)

Table 10 Global Post-Quantum Cryptography Market Outlook, By Integration & Deployment (2023-2034) (\$MN)

Table 11 Global Post-Quantum Cryptography Market Outlook, By Support & Maintenance (2023-2034) (\$MN)

Table 12 Global Post-Quantum Cryptography Market Outlook, By Algorithm Type (2023-2034) (\$MN)

Table 13 Global Post-Quantum Cryptography Market Outlook, By Lattice based (2023-2034) (\$MN)

Table 14 Global Post-Quantum Cryptography Market Outlook, By Code based (2023-2034) (\$MN)

Table 15 Global Post-Quantum Cryptography Market Outlook, By Multivariate (2023-2034) (\$MN)

Table 16 Global Post-Quantum Cryptography Market Outlook, By Hash based (2023-2034) (\$MN)

Table 17 Global Post-Quantum Cryptography Market Outlook, By Isogeny based (2023-2034) (\$MN)

Table 18 Global Post-Quantum Cryptography Market Outlook, By Deployment Mode

(2023-2034) (\$MN)

Table 19 Global Post-Quantum Cryptography Market Outlook, By On Premises

(2023-2034) (\$MN)

Table 20 Global Post-Quantum Cryptography Market Outlook, By Cloud (2023-2034)

(\$MN)

Table 21 Global Post-Quantum Cryptography Market Outlook, By Public Cloud

(2023-2034) (\$MN)

Table 22 Global Post-Quantum Cryptography Market Outlook, By Private Cloud

(2023-2034) (\$MN)

Table 23 Global Post-Quantum Cryptography Market Outlook, By Hybrid Cloud

(2023-2034) (\$MN)

Table 24 Global Post-Quantum Cryptography Market Outlook, By End User

(2023-2034) (\$MN)

Table 25 Global Post-Quantum Cryptography Market Outlook, By BFSI (2023-2034)

(\$MN)

Table 26 Global Post-Quantum Cryptography Market Outlook, By Government &

Defense (2023-2034) (\$MN)

Table 27 Global Post-Quantum Cryptography Market Outlook, By IT & Telecom

(2023-2034) (\$MN)

Table 28 Global Post-Quantum Cryptography Market Outlook, By Healthcare

(2023-2034) (\$MN)

Table 29 Global Post-Quantum Cryptography Market Outlook, By Retail & eCommerce

(2023-2034) (\$MN)

Table 30 Global Post-Quantum Cryptography Market Outlook, By Manufacturing

(2023-2034) (\$MN)

Table 31 Global Post-Quantum Cryptography Market Outlook, By Energy & Utilities

(2023-2034) (\$MN)

Table 32 Global Post-Quantum Cryptography Market Outlook, By Other End Users

(2023-2034) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Rest of the World (RoW) are also represented in the same manner as above.

I would like to order

Product name: Post-Quantum Cryptography Market Forecasts to 2034 – Global Analysis By Offering (Solutions and Services), Algorithm Type, Deployment Mode, End User and By Geography

Product link: <https://marketpublishers.com/r/P30465274F80EN.html>

Price: US\$ 4,150.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/P30465274F80EN.html>